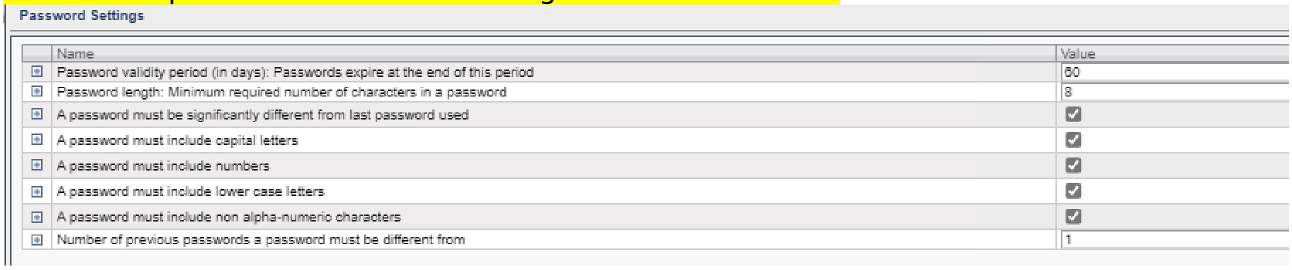
2. -Deafult password for admin changed ? MFA enabled ?

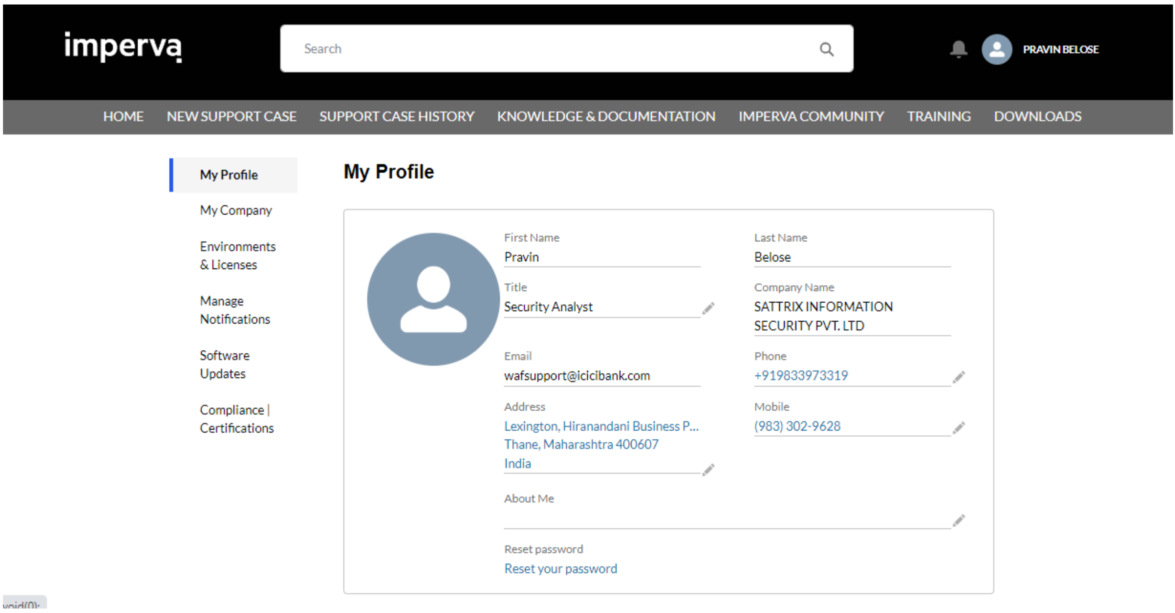


Password Settings

	Name	Value
⊞	Password validity period (in days): Passwords expire at the end of this period	60
⊞	Password length: Minimum required number of characters in a password	8
⊞	A password must be significantly different from last password used	☑
⊞	A password must include capital letters	☑
⊞	A password must include numbers	☑
⊞	A password must include lower case letters	☑
⊞	A password must include non alpha-numeric characters	☑
⊞	Number of previous passwords a password must be different from	1

6. - Any account configured for WAF OEM troubleshooting or assistance ?

6



My Profile

First Name: Pravin

Last Name: Belose

Title: Security Analyst

Company Name: SATTRIX INFORMATION SECURITY PVT. LTD

Email: wafsupport@icicibank.com

Phone: +919833973319

Address: Lexington, Hiranandani Business P...
Thane, Maharashtra 400607
India

Mobile: (983) 302-9628

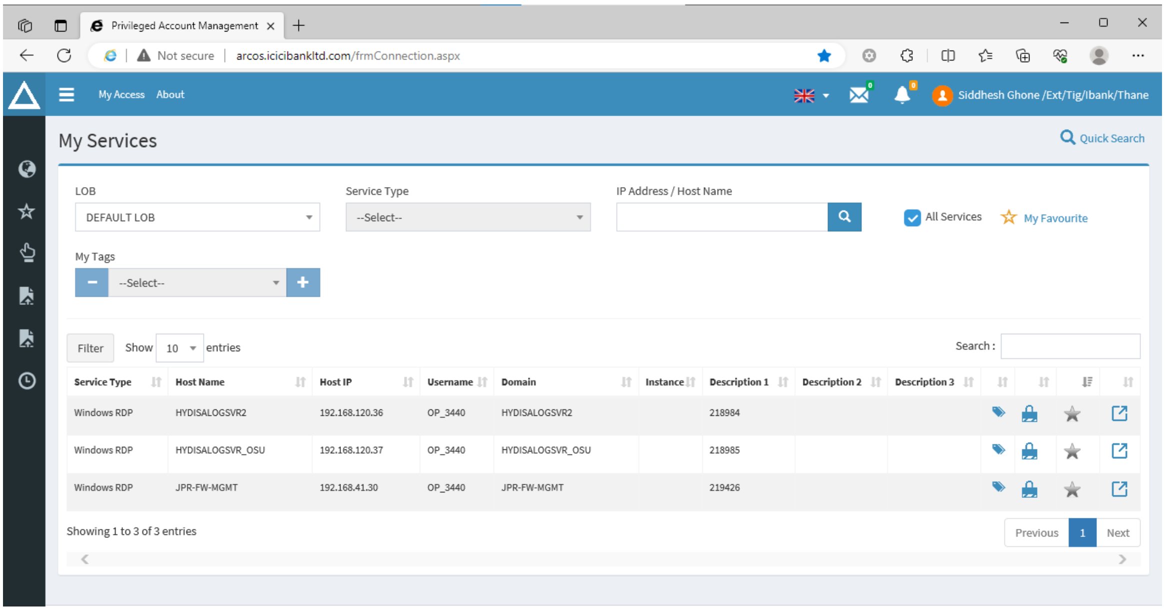
About Me

Reset password: Reset your password

void(0);

7. - Access to configuration changes is provided to whitelisted IPs only ?

For access to configuration changes we login through below mentioned server whitelisted IPs.



Privileged Account Management
Not secure
arcos.icicibankltd.com/frmConnection.aspx
My Access
About
Siddhesh Ghone /Ext/Tig/Ibank/Thane
Quick Search

My Services

LOB: DEFAULT LOB

Service Type: --Select--

IP Address / Host Name:

☑ All Services ☆ My Favourite

My Tags: --Select--

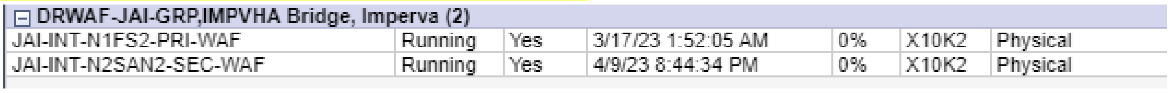
Filter Show 10 entries Search :

Service Type	Host Name	Host IP	Username	Domain	Instance	Description 1	Description 2	Description 3
Windows RDP	HYDISALOGSVR2	192.168.120.36	OP_3440	HYDISALOGSVR2		218984		
Windows RDP	HYDISALOGSVR_OSU	192.168.120.37	OP_3440	HYDISALOGSVR_OSU		218985		
Windows RDP	JPR-FW-MGMT	192.168.41.30	OP_3440	JPR-FW-MGMT		219426		

Showing 1 to 3 of 3 entries

Previous 1 Next

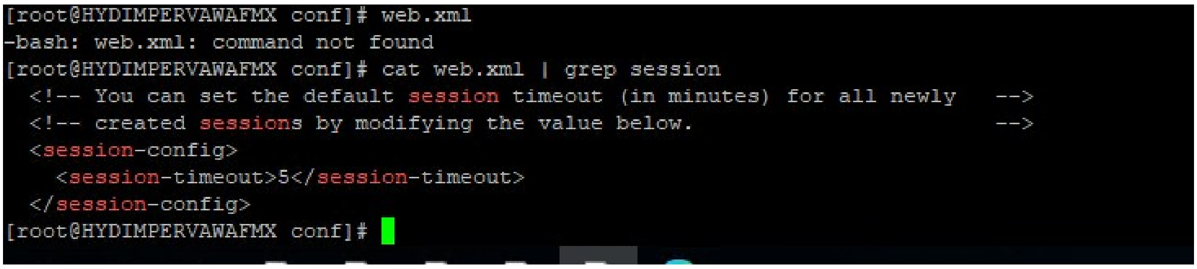
8. - Redundant server configured or not ?



⊟ DRWAF-JAI-GRP,IMPVHA Bridge, Imperva (2)

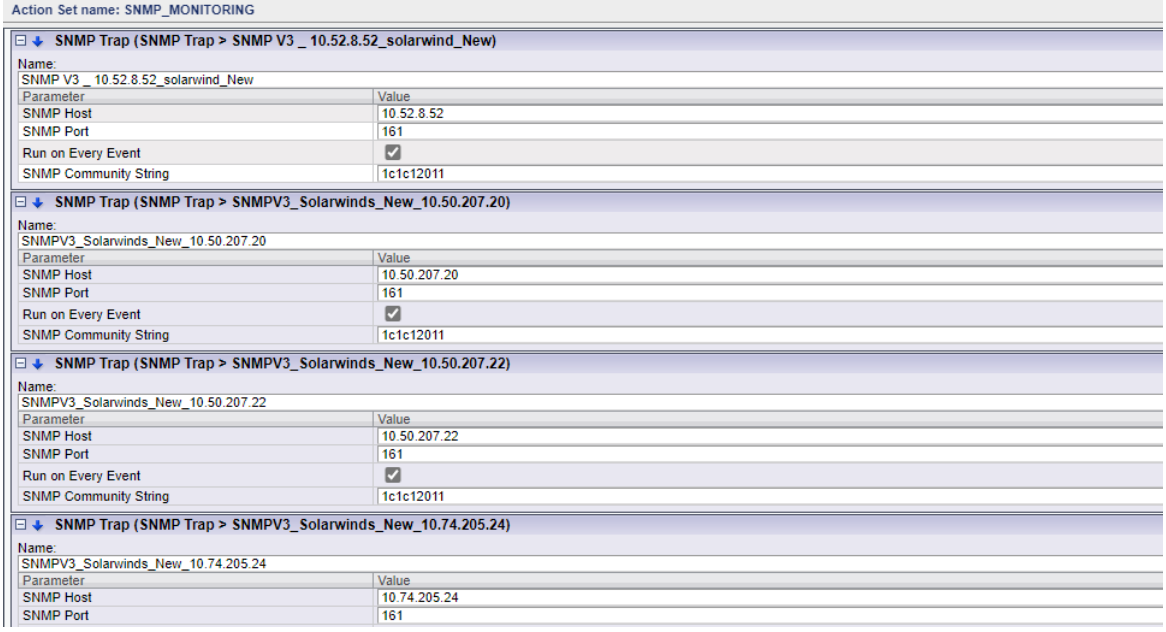
JAI-INT-N1FS2-PRI-WAF	Running	Yes	3/17/23 1:52:05 AM	0%	X10K2	Physical
JAI-INT-N2SAN2-SEC-WAF	Running	Yes	4/9/23 8:44:34 PM	0%	X10K2	Physical

9. - Timeout settings for session connections



```
[root@HYDIMPERVAWAFMX conf]# web.xml
-bash: web.xml: command not found
[root@HYDIMPERVAWAFMX conf]# cat web.xml | grep session
  <!-- You can set the default session timeout (in minutes) for all newly   -->
  <!-- created sessions by modifying the value below.                       -->
  <session-config>
    <session-timeout>5</session-timeout>
  </session-config>
[root@HYDIMPERVAWAFMX conf]#
```

12. - SNMP version and whitelisted IP ? Review frequency of whitelisted IP



Action Set name: SNMP_MONITORING

⊟ SNMP Trap (SNMP Trap > SNMP V3 _ 10.52.8.52_solarwind_New)

Name:
SNMP V3 _ 10.52.8.52_solarwind_New

Parameter	Value
SNMP Host	10.52.8.52
SNMP Port	161
Run on Every Event	☑
SNMP Community String	1c1c12011

⊟ SNMP Trap (SNMP Trap > SNMPV3_Solarwinds_New_10.50.207.20)

Name:
SNMPV3_Solarwinds_New_10.50.207.20

Parameter	Value
SNMP Host	10.50.207.20
SNMP Port	161
Run on Every Event	☑
SNMP Community String	1c1c12011

⊟ SNMP Trap (SNMP Trap > SNMPV3_Solarwinds_New_10.50.207.22)

Name:
SNMPV3_Solarwinds_New_10.50.207.22

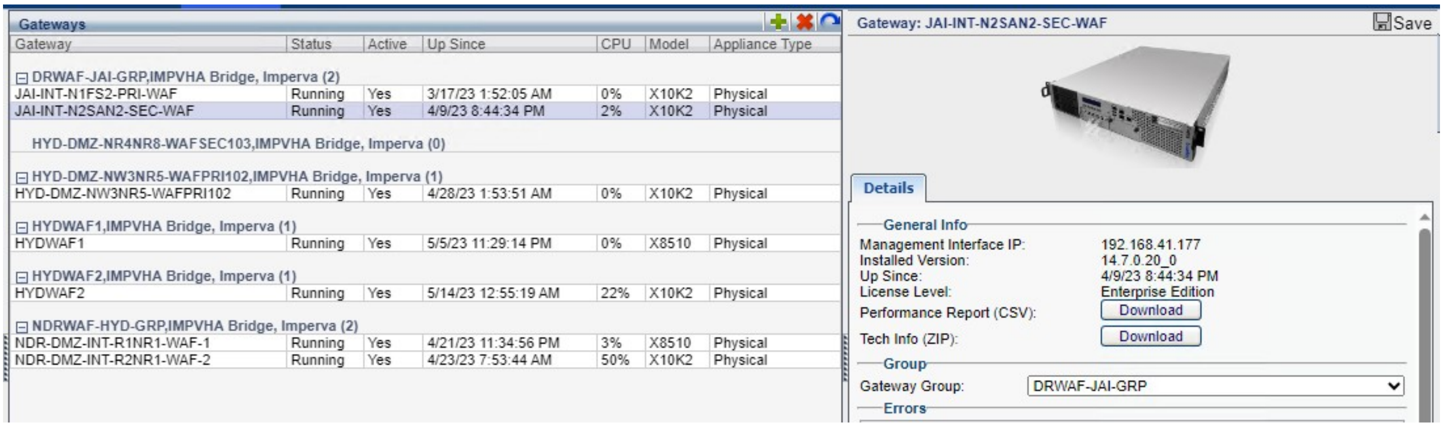
Parameter	Value
SNMP Host	10.50.207.22
SNMP Port	161
Run on Every Event	☑
SNMP Community String	1c1c12011

⊟ SNMP Trap (SNMP Trap > SNMPV3_Solarwinds_New_10.74.205.24)

Name:
SNMPV3_Solarwinds_New_10.74.205.24

Parameter	Value
SNMP Host	10.74.205.24
SNMP Port	161

15. - What is current OS version of WAF device?



Gateways

Gateway	Status	Active	Up Since	CPU	Model	Appliance Type
⊟ DRWAF-JAI-GRP,IMPVHA Bridge, Imperva (2)						
JAI-INT-N1FS2-PRI-WAF	Running	Yes	3/17/23 1:52:05 AM	0%	X10K2	Physical
JAI-INT-N2SAN2-SEC-WAF	Running	Yes	4/9/23 8:44:34 PM	2%	X10K2	Physical
HYD-DMZ-NR4NR8-WAFSEC103,IMPVHA Bridge, Imperva (0)						
⊟ HYD-DMZ-NW3NR5-WAFPRI102,IMPVHA Bridge, Imperva (1)						
HYD-DMZ-NW3NR5-WAFPRI102	Running	Yes	4/28/23 1:53:51 AM	0%	X10K2	Physical
⊟ HYDWAF1,IMPVHA Bridge, Imperva (1)						
HYDWAF1	Running	Yes	5/5/23 11:29:14 PM	0%	X8510	Physical
⊟ HYDWAF2,IMPVHA Bridge, Imperva (1)						
HYDWAF2	Running	Yes	5/14/23 12:55:19 AM	22%	X10K2	Physical
⊟ NDRWAF-HYD-GRP,IMPVHA Bridge, Imperva (2)						
NDR-DMZ-INT-R1NR1-WAF-1	Running	Yes	4/21/23 11:34:56 PM	3%	X8510	Physical
NDR-DMZ-INT-R2NR1-WAF-2	Running	Yes	4/23/23 7:53:44 AM	50%	X10K2	Physical

Gateway: JAI-INT-N2SAN2-SEC-WAF

General Info

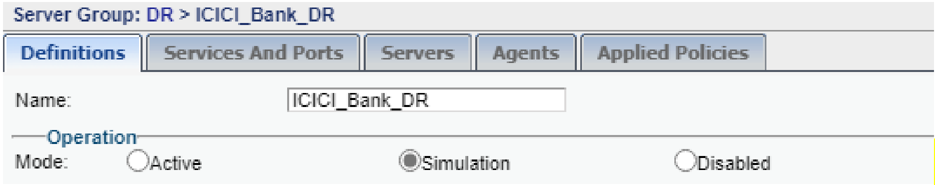
Management Interface IP:	192.168.41.177
Installed Version:	14.7.0.20_0
Up Since:	4/9/23 8:44:34 PM
License Level:	Enterprise Edition
Performance Report (CSV):	Download
Tech Info (ZIP):	Download

Group

Gateway Group: DRWAF-JAI-GRP

Errors

16. - Which mode is selected while onboarding application in WAF



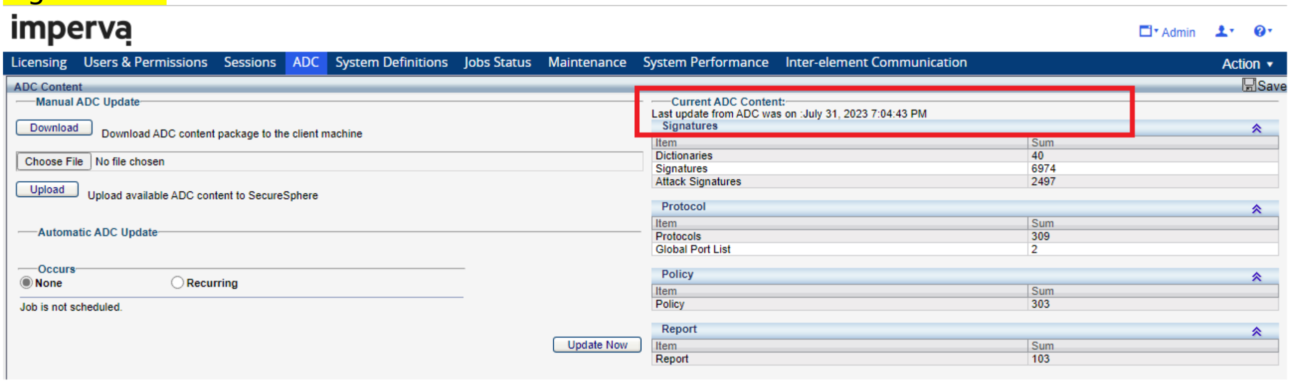
Server Group: DR > ICICI_Bank_DR

Name: ICICI_Bank_DR

Operation

Mode: ○ Active ● Simulation ○ Disabled

20.-How frequently WAF updates the signature ?



ADC Content

Manual ADC Update

Download — Download ADC content package to the client machine

Choose File — No file chosen

Upload — Upload available ADC content to SecureSphere

Automatic ADC Update

Occurs

● None ○ Recurring

Job is not scheduled.

Update Now

Current ADC Content:

Last update from ADC was on :July 31, 2023 7:04:43 PM

Signatures

Item	Sum
Dictionaries	40
Signatures	6974
Attack Signatures	2497

Protocol

Item	Sum
Protocols	309
Global Port List	2

Policy

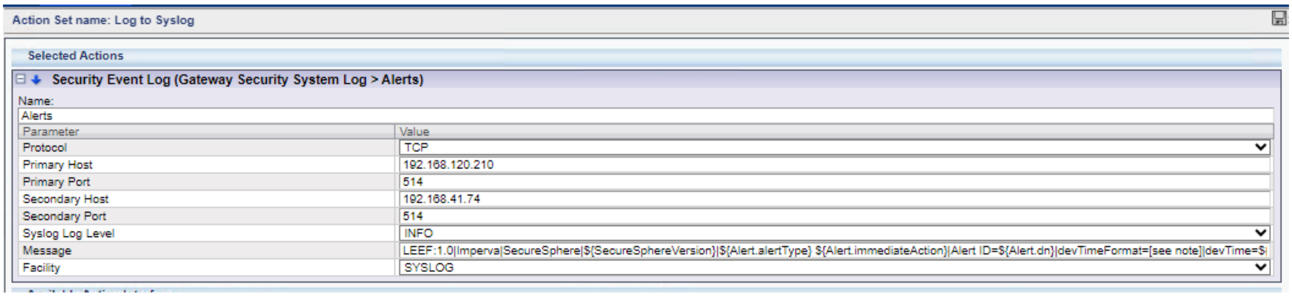
Item	Sum
Policy	303

Report

Item	Sum
Report	103

22. -Is WAF integrated with SIEM?

For Gateways



Action Set name: Log to Syslog

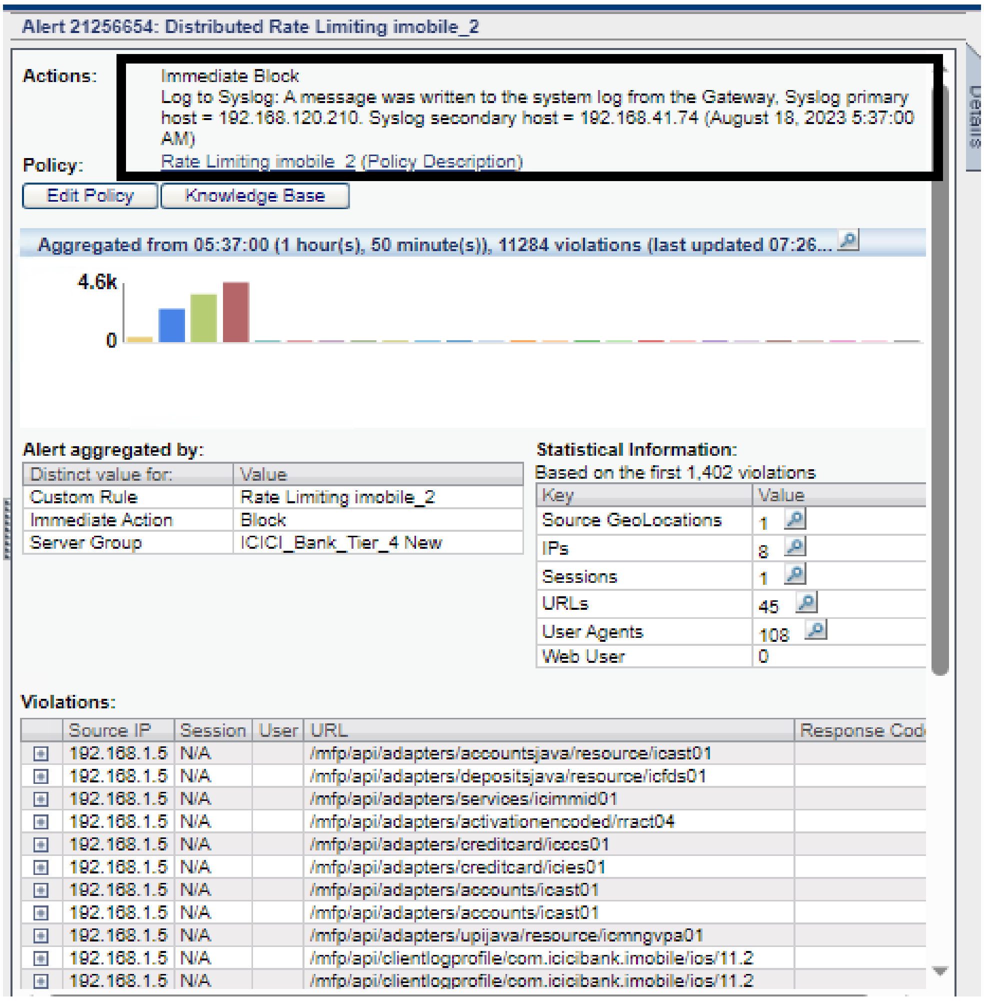
Selected Actions

Security Event Log (Gateway Security System Log > Alerts)

Name:
Alerts

Parameter	Value
Protocol	TCP
Primary Host	192.168.120.210
Primary Port	514
Secondary Host	192.168.41.74
Secondary Port	514
Syslog Log Level	INFO
Message	LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}\|${Alert.alertType} ${Alert.immediateAction}\|Alert ID=${Alert.dn}|devTimeFormat=[see note]|devTime=$|
Facility	SYSLOG

Evidence



Alert 21256654: Distributed Rate Limiting imobile_2

Actions: Immediate Block
Log to Syslog: A message was written to the system log from the Gateway. Syslog primary host = 192.168.120.210. Syslog secondary host = 192.168.41.74 (August 18, 2023 5:37:00 AM)

Policy: Rate Limiting imobile_2 (Policy Description)

Aggregated from 05:37:00 (1 hour(s), 50 minute(s)), 11284 violations (last updated 07:26...

Alert aggregated by:

Distinct value for:	Value
Custom Rule	Rate Limiting imobile_2
Immediate Action	Block
Server Group	ICICI_Bank_Tier_4 New

Statistical Information:
Based on the first 1,402 violations

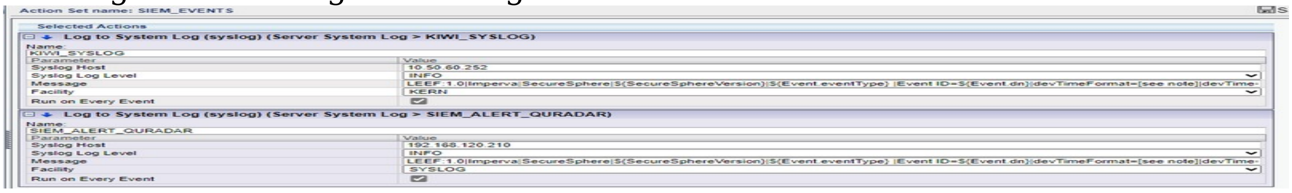
Key	Value
Source GeoLocations	1
IPs	8
Sessions	1
URLs	45
User Agents	108
Web User	0

Violations:

	Source IP	Session	User	URL	Response Cod
⊞	192.168.1.5	N/A		/mfp/api/adapters/accountsjava/resource/icast01	
⊞	192.168.1.5	N/A		/mfp/api/adapters/depositsjava/resource/icfds01	
⊞	192.168.1.5	N/A		/mfp/api/adapters/services/icimmid01	
⊞	192.168.1.5	N/A		/mfp/api/adapters/activationencoded/rract04	
⊞	192.168.1.5	N/A		/mfp/api/adapters/creditcard/icccs01	
⊞	192.168.1.5	N/A		/mfp/api/adapters/creditcard/icies01	
⊞	192.168.1.5	N/A		/mfp/api/adapters/accounts/icast01	
⊞	192.168.1.5	N/A		/mfp/api/adapters/accounts/icast01	
⊞	192.168.1.5	N/A		/mfp/api/adapters/upijava/resource/icmngvpa01	
⊞	192.168.1.5	N/A		/mfp/api/clientlogprofile/com.icicibank.imobile/ios/11.2	
⊞	192.168.1.5	N/A		/mfp/api/clientlogprofile/com.icicibank.imobile/ios/11.2	

23. -Is WAF Admin activity montioring in SIEM and the evidence

For Login and Configuration logs



Action Set name: SIEM_EVENTS

Selected Actions

Log to System Log (syslog) (Server System Log > KIWI_SYSLOG)

Name:
KIWI_SYSLOG

Parameter	Value
Syslog Host	10.50.60.252
Syslog Log Level	INFO
Message	LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}\|${Event.eventType} |Event ID=${Event.dn}|devTimeFormat=[see note]|devTime=
Facility	KERN
Run on Every Event	☑

Log to System Log (syslog) (Server System Log > SIEM_ALERT_QURADAR)

Name:
SIEM_ALERT_QURADAR

Parameter	Value
Syslog Host	192.168.120.210
Syslog Log Level	INFO
Message	LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}\|${Event.eventType} |Event ID=${Event.dn}|devTimeFormat=[see note]|devTime=
Facility	SYSLOG
Run on Every Event	☑

Evidence

Need to atach configuration change log(get from SIEM team and attach).

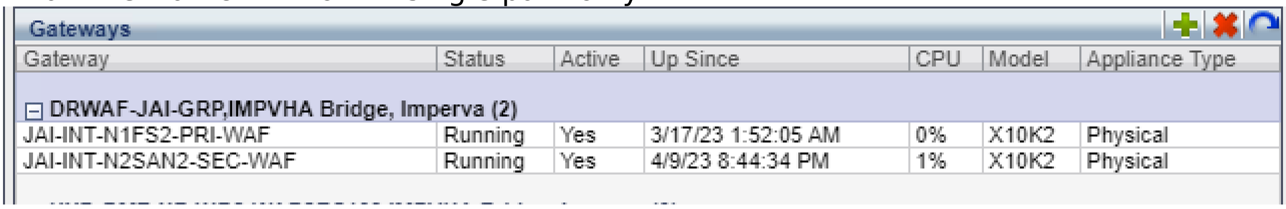
24. -Is any application attack monitored in SIEM and its evidence

Yes, The attacks are monitored in SIEM.

Need to atach any alert log from SIEM side(get from SIEM team and attach).

26. -How WAF is configured? Active - Active or Active - Passive

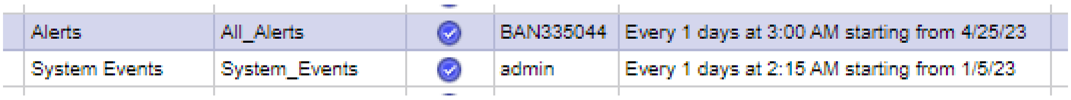
At a time traffic will flow in single path only.



Gateways

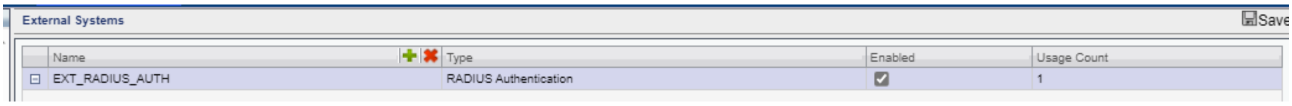
Gateway	Status	Active	Up Since	CPU	Model	Appliance Type
⊟ DRWAF-JAI-GRP,IMPVHA Bridge, Imperva (2)						
JAI-INT-N1FS2-PRI-WAF	Running	Yes	3/17/23 1:52:05 AM	0%	X10K2	Physical
JAI-INT-N2SAN2-SEC-WAF	Running	Yes	4/9/23 8:44:34 PM	1%	X10K2	Physical

28. -Is any schedule reports are configure?



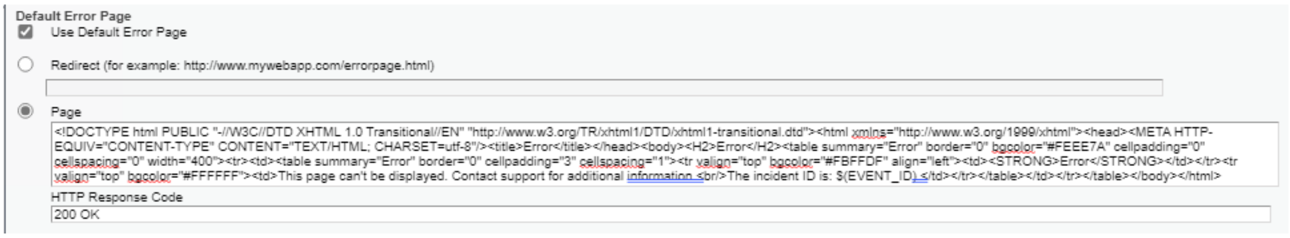
Alerts	All_Alerts	✓	BAN335044	Every 1 days at 3:00 AM starting from 4/25/23
System Events	System_Events	✓	admin	Every 1 days at 2:15 AM starting from 1/5/23

29. -Is WAF integrated with AD ?



	Name	Type	Enabled	Usage Count
⊟	EXT_RADIUS_AUTH	RADIUS Authentication	☑	1

30. -What error page is displayed by WAF?



Default Error Page

☑ Use Default Error Page

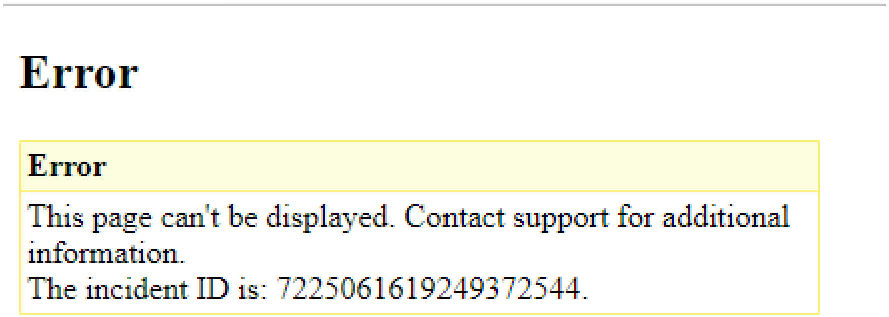
○ Redirect (for example: http://www.mywebapp.com/errorpage.html)

● Page

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="TEXT/HTML; CHARSET=utf-8"/><title>Error</title></head><body><H2>Error</H2><table summary="Error" border="0" bgcolor="#FEEE7A" cellpadding="0" cellspacing="0" width="400"><tr><td><table summary="Error" border="0" cellpadding="3" cellspacing="1"><tr valign="top" bgcolor="#FBFFDF" align="left"><td><STRONG>Error</STRONG></td></tr><tr valign="top" bgcolor="#FFFFFF"><td>This page can't be displayed. Contact support for additional information.<br/>The incident ID is: $(EVENT_ID).</td></tr></table></td></tr></table></body></html>
```

HTTP Response Code

200 OK



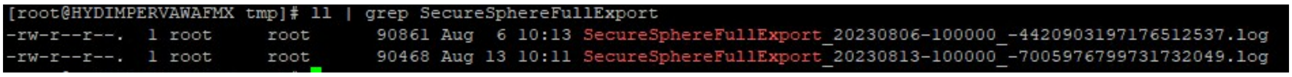
Error

Error

This page can't be displayed. Contact support for additional information.

The incident ID is: 7225061619249372544.

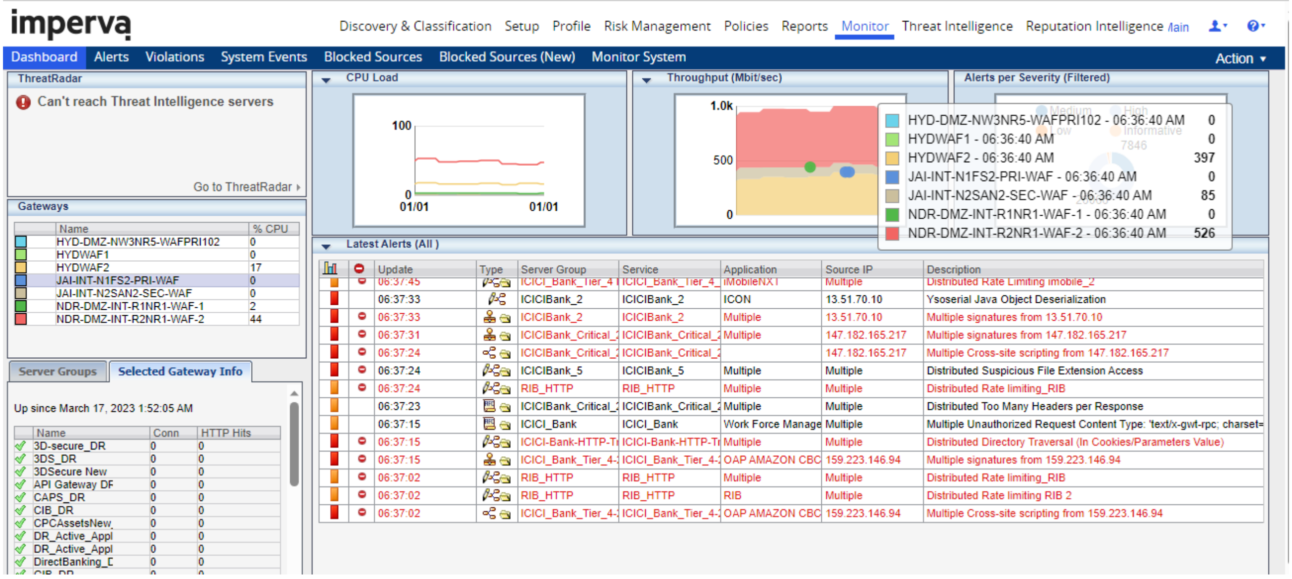
31. -WAF configuration backup is happening and how frequent?



```
[root@HYDIMPERVAWAFMX tmp]# ll | grep SecureSphereFullExport
-rw-r--r--.  1 root      root      90861 Aug  6 10:13 SecureSphereFullExport_20230806-100000_-4420903197176512537.log
-rw-r--r--.  1 root      root      90468 Aug 13 10:11 SecureSphereFullExport_20230813-100000_-7005976799731732049.log
```

33. -How WAF health and resource utilization is monitored ?

Gateway



ThreatRadar

Can't reach Threat Intelligence servers

Go to ThreatRadar ›

Gateways

	Name	% CPU
🟦	HYD-DMZ-NW3NR5-WAFPRI102	0
🟩	HYDWAF1	0
🟨	HYDWAF2	17
🟦	JAI-INT-N1FS2-PRI-WAF	0
▨	JAI-INT-N2SAN2-SEC-WAF	0
🟩	NDR-DMZ-INT-R1NR1-WAF-1	2
🟥	NDR-DMZ-INT-R2NR1-WAF-2	44

Server Groups | Selected Gateway Info

Up since March 17, 2023 1:52:05 AM

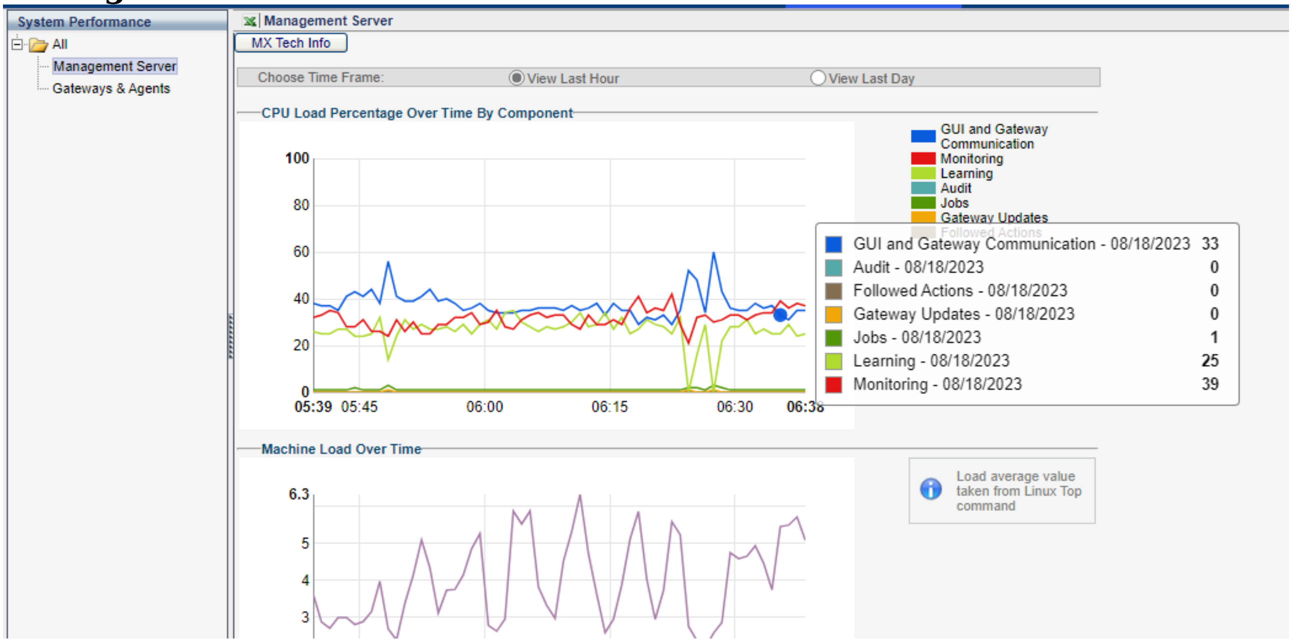
	Name	Conn	HTTP Hits
✓	3D-secure_DR	0	0
✓	3DS_DR	0	0
✓	3DSecure New	0	0
✓	API Gateway DF	0	0
✓	CAPS_DR	0	0
✓	CIB_DR	0	0
✓	CPCAssetsNew_	0	0
✓	DR_Active_Appl	0	0
✓	DR_Active_Appl	0	0
✓	DirectBanking_[	0	0
✓	CIB_DR	0	0

🟦 HYD-DMZ-NW3NR5-WAFPRI102 - 06:36:40 AM	0
🟩 HYDWAF1 - 06:36:40 AM	0
🟨 HYDWAF2 - 06:36:40 AM	397
🟦 JAI-INT-N1FS2-PRI-WAF - 06:36:40 AM	0
▨ JAI-INT-N2SAN2-SEC-WAF - 06:36:40 AM	85
🟩 NDR-DMZ-INT-R1NR1-WAF-1 - 06:36:40 AM	0
🟥 NDR-DMZ-INT-R2NR1-WAF-2 - 06:36:40 AM	526

Latest Alerts (All)

		Update	Type	Server Group	Service	Application	Source IP	Description
🟧	⛔	06:37:45		ICICI_Bank_Tier_4	ICICI_Bank_Tier_4_	iMobileNXT	Multiple	Distributed Rate Limiting imobile_2
🟥		06:37:33		ICICIBank_2	ICICIBank_2	ICON	13.51.70.10	Ysoserial Java Object Deserialization
🟥	⛔	06:37:33		ICICIBank_2	ICICIBank_2	Multiple	13.51.70.10	Multiple signatures from 13.51.70.10
🟥	⛔	06:37:31		ICICIBank_Critical_	ICICIBank_Critical_	Multiple	147.182.165.217	Multiple signatures from 147.182.165.217
🟥	⛔	06:37:24		ICICIBank_Critical_	ICICIBank_Critical_		147.182.165.217	Multiple Cross-site scripting from 147.182.165.217
🟥	⛔	06:37:24		ICICIBank_5	ICICIBank_5	Multiple	Multiple	Distributed Suspicious File Extension Access
🟧	⛔	06:37:24		RIB_HTTP	RIB_HTTP	Multiple	Multiple	Distributed Rate limiting_RIB
🟧		06:37:23		ICICIBank_Critical_	ICICIBank_Critical_	Multiple	Multiple	Distributed Too Many Headers per Response
🟧		06:37:15		ICICI_Bank	ICICI_Bank	Work Force Manage	Multiple	Multiple Unauthorized Request Content Type: 'text/x-gwt-rpc; charset=
🟥	⛔	06:37:15		ICICI-Bank-HTTP-Ti	ICICI-Bank-HTTP-Ti	Multiple	Multiple	Distributed Directory Traversal (In Cookies/Parameters Value)
🟥	⛔	06:37:15		ICICI_Bank_Tier_4-	ICICI_Bank_Tier_4-	OAP AMAZON CBC	159.223.146.94	Multiple signatures from 159.223.146.94
🟧	⛔	06:37:02		RIB_HTTP	RIB_HTTP	Multiple	Multiple	Distributed Rate limiting_RIB
🟧	⛔	06:37:02		RIB_HTTP	RIB_HTTP	RIB	Multiple	Distributed Rate limiting RIB 2
🟥	⛔	06:37:02		ICICI_Bank_Tier_4-	ICICI_Bank_Tier_4-	OAP AMAZON CBC	159.223.146.94	Multiple Cross-site scripting from 159.223.146.94

Management



Choose Time Frame: ● View Last Hour ○ View Last Day

🟦 GUI and Gateway Communication - 08/18/2023	33
🟦 Audit - 08/18/2023	0
🟫 Followed Actions - 08/18/2023	0
🟧 Gateway Updates - 08/18/2023	0
🟩 Jobs - 08/18/2023	1
🟩 Learning - 08/18/2023	25
🟥 Monitoring - 08/18/2023	39

Load average value taken from Linux Top command